

- - Transmitters/Receivers of Long -Range Echelon
- - Receivers of Central and Short-Range Echelons

2011

Alternative sequences of detected signals in echelons			Versions of intrusion in eshelons			Versions of self-checking results	Notes
C	S	L	Ingress	Egress	Presence inside		
C →▷C					+	May also mean an unauthorized discloser of protected housing.	Emitted ultrasound goes outside.
C →▷S				+		Target moves to echelon L ? Check it.	
S →▷C			+			Target moves from echelon L ? Check it. Echelon L may be in the failed state.	
C →▷L				+		Target moves inside echelon L ? Check it. Echelon S may be in the failed state.	
L →▷C			+			Target moves inside echelon C ? Check it. Echelon S may be in the failed state.	
	S →▷S				+	Target moves in echelon S? Check it. Other echelons C and L may be in the failed state.	
	S →▷L			+		Target moves from echelon C ? Check it. Echelon C may be in the failed state.	
	L →▷S		+			Target moves to echelon C? Check it. Echelon C may be in the failed state.	
		L →▷L			+	Target moves inside echelon L ? Check it. An intruder may not be threat if it passes by the echelon S.	
<b>Note:</b> Arrows show the directional sequence of caution signals from intrusion-suspected echelons.							

FIG. 3

Sublevels of echelons (in indices of FIG.3)	L <sub>1</sub>	L <sub>2</sub>	L <sub>3</sub>	L <sub>4</sub>	S <sub>1</sub>	S <sub>2</sub>	S <sub>3</sub>	S <sub>4</sub>	S <sub>5</sub>	C <sub>1</sub>	C <sub>2</sub>	C <sub>3</sub>	Expected sequent events and real menaces at single intrusion
L <sub>1</sub>	X												VAM, PO, OCF, CCF.
L <sub>2</sub>		X											VAM, PO, OCF, CCF.
L <sub>3</sub>			X										VAM, PO, OCF, CCF.
L <sub>4</sub>				X					X				VAM, PO, OCF, CCF.
S <sub>1</sub>					X					X			VAM, OCF.
S <sub>2</sub>	X					X							VAM, IF.
S <sub>3</sub>					X		X					X	VAM, LF.
S <sub>4</sub>				X				X					VAM, CCF.
S <sub>5</sub>		X				X			X				VAM, CCF.
C <sub>1</sub>	X		X		X		X	X		X	X		VAM, SSF.
C <sub>2</sub>											X		VAM, CCF.
C <sub>3</sub>							X					X	VAM, SSF, CCF.
Expected sequent events and real menaces at multiple intrusion	CCF	CCF	PO, DF	PO, DF	IF, DF	DF	DF, SSF	SSF CCF	LF, SCF	LF, DF	CCF	DF, PO	<i>The pre- designed samples of vulnerability of surveyed areas are being kept in archive data file.</i>

FIG. 4

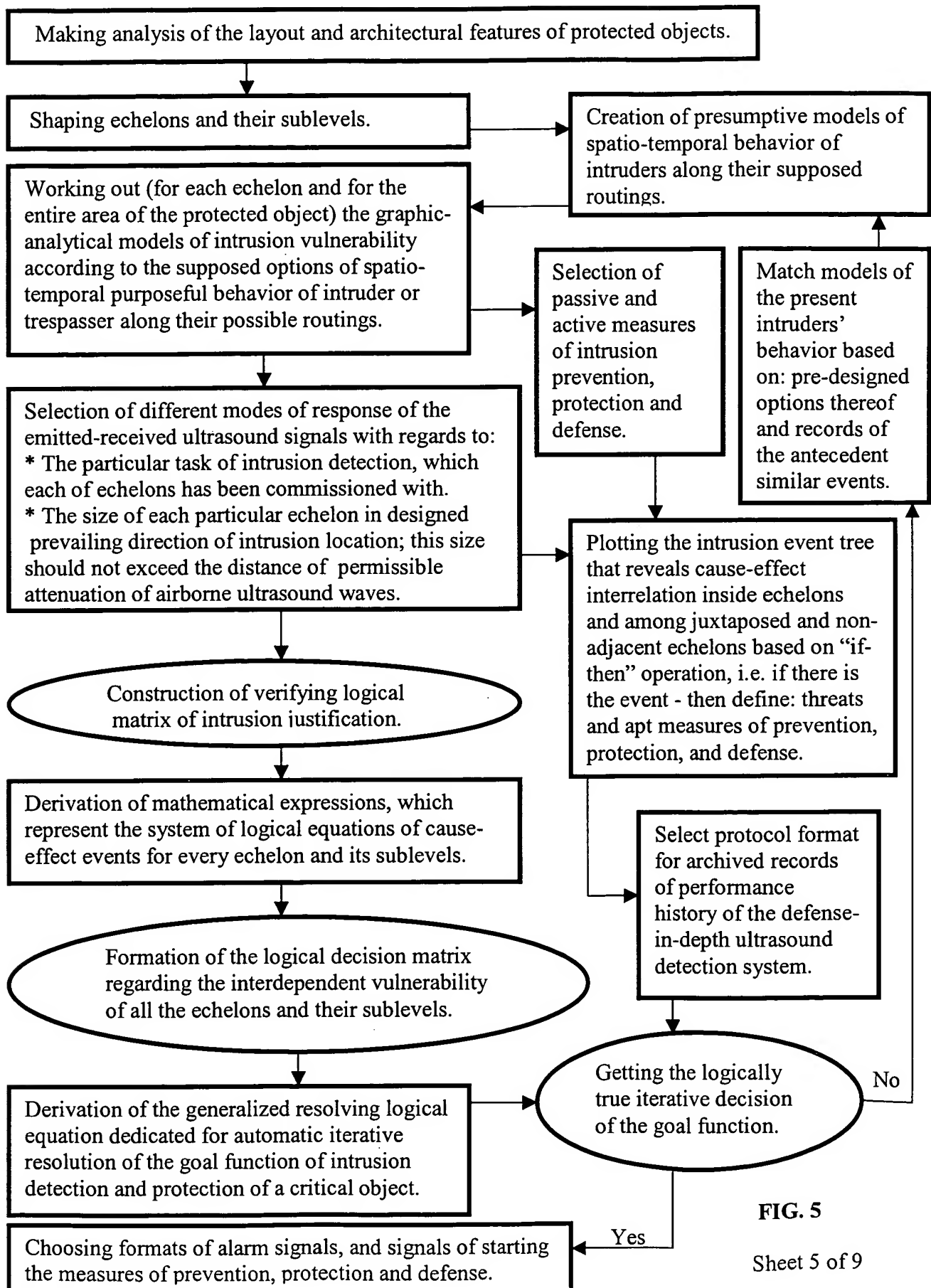
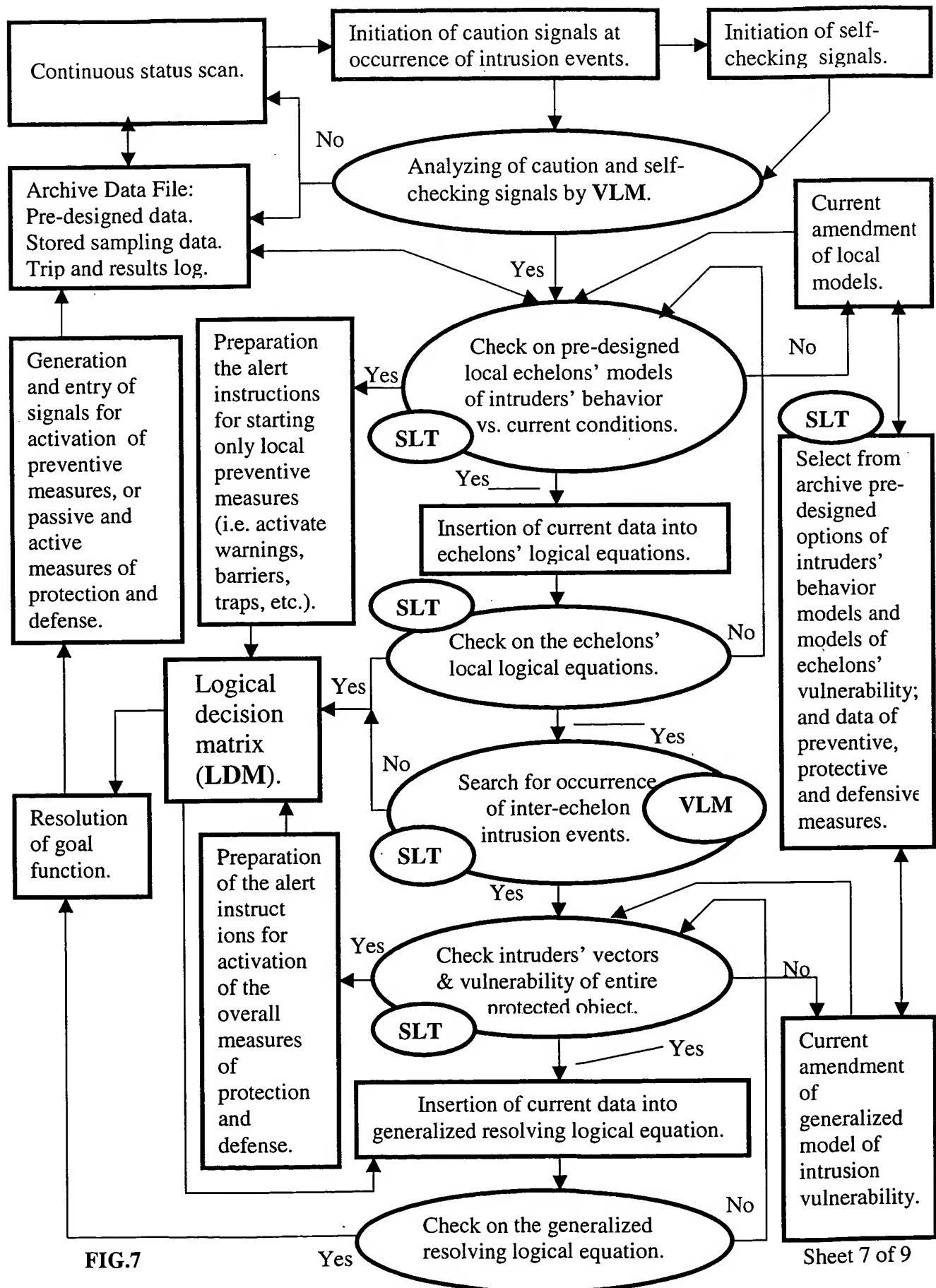


FIG. 5

<b>Data Files of Operative Algorithm</b>	<b>Stages of System's Design and Operation</b>	<b>Data Record and Input Format</b>	<b>Data Processing Formats and Modes</b>	<b>Note</b>
Preetermined Design Data	Design of multi-echelon arrangement of ultrasound detection system. Definition of its adjustment and starting-up basics.	Models of echelons' and entire protected area's intrusion vulnerability based on the presumptive models of intruders' run.	Optional spatio-temporal routings of intruders with cause-effect evaluation of vulnerability of facilities and the whole of object.	The size of each echelon is being rated in accordance with airborne ultrasound wave attenuation along its incidence-reflection trip.
Data batch entry under commissioning:	Evaluation of cause-effect intrusion menaces and potential vulnerabilities.	Intrusion event tree that represents cause-effect interdependent menaces among echelons.	The event tree in tabular or flow-chart format based on the "if-then" operation.	The properly selected modes of response of emitted ultrasound signals predict the sequent correct determination of cause-effect intrusion events.
Data batch entry during operation:	Plotting spatio-temporal data of intrusion routings.	Analysis of modeled and running intrusion data.	Look-up table of modeled previously and current data of intrusion menaces.	
Informational and Processing Inter-echelon Interrelation	Vindication of single or group intrusion detection signals. Accomplishment of final, logically true decision of goal function of intrusion detection and protection.	Entry of caution and self-checking signals into verifying logical matrix. Iterative resolution of the goal function during continuous status scan and data acquisition.	Entry of resulted data of treatment of caution and self-checking signals into: local logical equations of echelons, logical decision matrix and generalized resolving logical equation.	The current operation of system's data control block provides for data acquisition (in particular: caution and self-checking signals) due to continuous status scan of all detectors.
Intermediate derived data:	The decisions of: logical equation of each echelon; logical decision matrix. The decision of generalized resolving logical equation.	The menaces of echelons and their sublevels, and entire threat to the object. The resolution of goal function of protection.	Data of continuous status scan input into any logical equation and into logical decision matrix only thru verifying logical matrix.	The verifying logical matrix analyses all caution and self-checking signals to avoid fault resolutions of the goal function.
Finalized derived data: Executive and Actual Instructions	Generation and entry of alarm signals and signals for actuation measures of prevention, protection and defense.	Entry of instructions for: Start of local preventive measures; and Carrying out passive and active measures of final protection and defense.	Preferably the preventive local measures include entry of warning signals, actuation of barriers and entrapments against an intruding subject.	Alarm signals are being represented in the result of justification of caution signals for really effected echelon by the verifying logical matrix.
Trip and Results Log	Sampling and archiving the historical files of safety and security maintenance.	Continuous archiving all the samples of operating status of the system.	Informational archive data transferring goes in the two-way exchange mode.	Use from archive data file the antecedent resolutions of the goal function.

**FIG. 6**



Indices of echelons and sublevels therein	Event occurrence logical equation	Factors of menaces in the order of diminishing rate	Pre-designed selective security measures
<b>L<sub>1</sub></b>	$L_1 + (L_1 \cdot S_2) + (L_1 \cdot C_1) = \text{High level threat (HT)}$	$(PO + OCF + CCF) \cdot VAM$	VAM + PO, → Intrusion prevention and start backup power. Other menaces, → Measures of intrusion protection and defense.
<b>L<sub>2</sub></b>	$L_2 + (L_2 \cdot S_5) = \text{High level threat (HT)}$	$(CCF + OCF + PO) \cdot VAM$	The same as for L <sub>1</sub> .
<b>L<sub>3</sub></b>	$L_3 + (L_3 \cdot C_1) = \text{Low level threat (LT)}$	$(PO + DP) \cdot VAM$	Intrusion prevention : activate backup power, warnings, barriers, etc.
<b>L<sub>4</sub></b>	$L_4 + (L_4 \cdot S_4) = \text{LT}$	$(PO + DP) \cdot VAM$	Intrusion prevention : activate backup power, warnings, barriers, etc.
<b>L</b>	$(L_1 + L_2 + L_3 + L_4) + (L_1 \cdot L_2 \cdot L_3 \cdot L_4) = \text{HT}$	$(CCF + PO + OCF) \cdot VAM$	Selective activation of intrusion prevention, protection and defense.
<b>S<sub>1</sub></b>	$S_1 + (S_1 \cdot S_3) + (S_1 \cdot C_1) = \text{LT}$	$(DF + IF) \cdot VAM$	Intrusion prevention : activate barriers, traps, redundant blocks, etc.
<b>S<sub>2</sub></b>	$S_2 + (S_2 \cdot S_5) = \text{LT}$	$DF \cdot VAM$	Intrusion prevention : activate barriers, traps, redundant blocks, etc.
<b>S<sub>3</sub></b>	$S_3 + (S_3 \cdot C_1) + (S_3 \cdot C_3) = \text{Moderate level threat (MT)}$	$(SSF + DF) \cdot VAM$	Selective activation of intrusion prevention, protection and defense.
<b>S<sub>4</sub></b>	$S_4 + (S_4 \cdot C_1) = \text{HT}$	$(CCF + SSF) \cdot VAM$	Passive and active measures of intrusion protection and defense.
<b>S<sub>5</sub></b>	$S_5 + (S_5 \cdot L_4) = \text{MT}$	$[(LF + SCF) \cdot VAM] + [(LF \cdot SCF) \cdot VAM]$	Selective activation of intrusion prevention, protection and defense.
<b>S</b>	$(S_1 + S_2 + S_3 + S_4 + S_5) + (S_1 \cdot S_2 \cdot S_3 \cdot S_4 \cdot S_5) = \text{HT}$	$\{[CCF + (SSF + DF + LF + SCF + IF)] + [(SCF \cdot LF) + (SSF \cdot DF) + SCF]\} \cdot VAM$	Selective activation of intrusion prevention, protection and defense.
<b>C<sub>1</sub></b>	$C_1 + (C_1 \cdot S_1) = \text{MT}$	$\{[SSF \cdot (LF + DF)] + [(SSF \cdot LF \cdot DF)]\} \cdot VAM$	Selective activation of intrusion prevention, protection and defense.
<b>C<sub>2</sub></b>	$C_2 + (C_2 \cdot C_1) = \text{HT}$	$CCF \cdot VAM$	Passive and active measures of intrusion protection and defense.
<b>C<sub>3</sub></b>	$C_3 + (C_3 \cdot S_3) = \text{HT}$	$[CCF + (CCF \cdot SSF) + (CCF \cdot DF) + (CCF \cdot PO) + (SSF \cdot DF) + (SSF \cdot PO)] \cdot VAM$	Passive and active measures of intrusion protection and defense.
<b>C</b>	$(C_1 + C_2 + C_3) + (C_1 \cdot C_2 \cdot C_3) = \text{HT}$	$\{CCF + [(CCF \cdot SSF) + (SSF \cdot DF) + (LF \cdot DF)] \cdot PO\} \cdot VAM$	Selective activation of intrusion prevention, protection and defense.
<b>GRLE</b>	$[(L \cdot S) + (S \cdot C) + (L \cdot S \cdot C)] + [(L \cdot C) + (C \cdot S) + (C \cdot S \cdot L)] = \text{HT}$	$\{[(CCF + (CCF \cdot SSF) + (LF \cdot OCF) + (SSF \cdot SCF) + (SSF \cdot DF \cdot IF))] \cdot PO\} \cdot VAM$	Passive and active measures of intrusion protection and defense.

FIG.8



